AMENDMENT TO CLAIMS

Please amend claims 1-3, all as shown below. All pending claims are reproduced below, including those that remain unchanged. Claims 33-49 have been renumbered as 4-20.

1. (Currently amended) A machine system for protecting access constrained information from unauthorized access by way of unauthorized users or unauthorized programs, said machine system comprising:

(a) data-providing means for providing data of an identified one of two or more digital data files, where each of said files is identifiable by a file name and where each of said files is stored and retrievable ~~from~~ either ~~a local storage~~ locally or remotely ~~from an external storage~~;

(b) an interceptable access mechanism through which data of an identified file of the data-providing means is accessed by identifiable, access-requesting programs and/or access-requesting users;

(c) access-control means coupled to intercept data access attempts made through said interceptable access mechanism,

(c.1) wherein the access-control means includes deny/approve means for testing the intercepted data access attempts and responsively denying or approving intelligible or other data access to the data of an identified subset of said files based on one or more of the identity of an access-attempting program, the time of the access attempt, the machine or location from which the access request originates and a user associated with the access request, and

(c.2) wherein the access-control means includes permissions control means for responding to permission rules associated with respective ones of identifiable subsets of said files; and

(d) localizing means for transparently and temporarily localizing external files and respective external permission rules of such external files for use by said access-control means.

2. (Currently amended) A machine-implemented method for protecting access constrained information from unauthorized access by way of unauthorized users or unauthorized programs, said machine-implemented method comprising:

(a) in response to a navigation-based request, providing data of an identified one of two or more digital data files, where each of said files is identified in the navigation-based request by a file name, file handle, or equivalent and where each of said files is stored and retrievable ~~from~~ either ~~a local storage~~ locally or remotely ~~from an external storage~~;

(b) intercepting data access attempts made through an interceptable access mechanism, wherein:

(b.1) the interceptable access mechanism is one through which data of an identified file of the data-providing means is accessed by identifiable, access-requesting programs and/or access-requesting users;

(b.2) the interceptable access mechanism includes access-control means includes deny/approve means for testing the intercepted data access attempts and responsively denying or approving intelligible or other data access to the data of an identified subset of said files based on one or more of the identity of an access-attempting program, the time of the access attempt, the machine or location from which the access request originates and a user associated with the access request, and

(b.3) the access-control means includes permissions control means for responding to permission rules associated with respective ones of identifiable subsets of said files; and said method further comprises:

(c) in response to those of said navigation-based requests which request external files, transparently and temporarily localizing the external files and the respective external permission rules of such external files for use by said access-control means.

3. (Currently amended) The machine-implemented protecting method of Claim 2 wherein:

confidential information is kept ~~essentially and~~ consistently in encrypted format when the confidential information either resides within a remote file server or within easily removable media or when such confidential information is in-transit along an untrusted (not-secure) communications link;

said confidential information is exposed in plaintext form on an as-needed and as-authorized basis, essentially only when said confidential information resides within a local client that is conveniently viewable by one or more authorized users;

said plaintext exposure is allowed to occur only after an authorized user validates his or her authorization to access the information at the local client.

Claims 4-32 have been withdrawn.

4. (Original) An instruction conveying means for instructing an instructable machine to carry out an access-constraining method for files that primarily reside either inside or outside the instructable machine, where the instructable machine has an internal, data-providing means that can provide data from an identified one of internal or external, plural digital data files in response to interceptable file-access requests, where each of said files is identifiable by a file name, said machine-implemented, access-constraining method being for protecting data and/or information of said files from unauthorized access by way of unauthorized ones of identifiable programs and/or at the behest of unauthorized, identifiable users, said internal/external access-constraining method comprising:

(a) intercepting data access attempts made by access requesting programs for data in an identified one of files residing primarily on an identified internal, removable, or external media;

(b) first testing for each intercepted data access attempt, to verify that the identified media on which the requested file primarily resides is currently available, and if not, updating local records which track the current availability of the identified media to indicate the current non-availability of the media;

(c) second testing for each intercepted data access attempt, to determine if access constraining control information is already available internally for the identified file;

(d) if said second testing shows that the access constraining control information is not available in an internal and physically-secure storage area, attempting to securely import the missing, access constraining control information from the removable, or external media of primary residence of the identified file;

(e) if said import attempt shows that the missing, access constraining control information is unavailable, determining explicitly or implicitly if the missing information is necessary for allowing the intercepted access-request to complete normally to provide a grant of the request, and if the missing information is necessary, blocking the intercepted access-request from

completing normally and thereby blocking the provision of said grant in response to the intercepted access-request.

5. (Original) The instructions conveying means of Claim 33 and further wherein said step (d) of attempting to securely import the missing, access constraining control information includes at least one of:

(d.1) verifying a digital signature covering corresponding access constraining control information that is held in said removable, or external media of primary residence of the identified file and imported into said instructable machine;

(d.2) decrypting imported digital data that represents the corresponding access constraining control information of the identified file; and

(d.3) storing a digital-signature authenticated and/or decrypted, plaintext version of the missing, access constraining control information in said internal and physically-secure storage area of the instructable machine.

6. (Original) The instructions conveying means of Claim 33 and wherein said internal/external access-constraining method further comprises:

(f) third testing for each intercepted data access attempt, to determine if the identified file is an access constrained one which resides primarily on removable, or external media, and if so to determine whether a localized copy of the identified file is present in the instructable machine;

(g) if said third testing shows that the localized copy is not present, importing a copy of the identified file into said internal and physically-secure storage area of the instructable machine.

7. (Original) The instructions conveying means of Claim 35 and wherein said internal/external access-constraining method further comprises:

(h) recording the time of said importing of the copy of the identified file so that said time of localization can be later used by garbage collection mechanisms of the instructable machine to remove localized copies that have remained localized beyond a predefined time limit.

8. (Original) The instructions conveying means of Claim 35 and wherein said internal/external access-constraining method further comprises:

(h) determining if the just-localized file copy imported in step (g) is one whose primary data is encrypted;

(i) attempting to decrypt the encrypted primary data of the just-localized file copy if the determining step (h) shows that such encrypted data is present; and

(j) blocking the intercepted access-request from completing normally and thereby blocking the provision of said grant in response to the intercepted access-request if the attempted decryption of step (i) is unsuccessful.

9. (Original) The instructions conveying means of Claim 37 and wherein said internal/external access-constraining method further comprises:

(k) attempting to verify a digital signature covering the decrypted primary data of step (i); and

(l) blocking the intercepted access-request from completing normally and thereby blocking the provision of said grant in response to the intercepted access-request if the signature verification of step (k) is unsuccessful.

10. (Original) The instructions conveying means of Claim 37 and wherein said internal/external access-constraining method further comprises:

(k) volume encrypting the decrypted primary data of step (i) and storing the volume encrypted data to nonvolatile storage;

wherein the decrypted primary data is kept within the instructable machine exclusively in volatile storage thereof.

11. (Original) An instructions conveying means for instructing an instructable machine to carry out an nonresident file-closing method for files that primarily reside removably or outside the instructable machine, where the instructable machine has an internal, data-providing means that can provide data from an identified one of internal or external, plural digital data files in response to interceptable file-open requests, where each of said files is identifiable by a file name, said machine-implemented, file-closing method being for protecting

data and/or information of said nonresident files from unauthorized access by way of unauthorized ones of identifiable programs and/or at the behest of unauthorized, identifiable users, said nonresident file-closing method comprising:

(a) intercepting file-closing attempts made by access-completing parts of access-requesting programs, where the original access requests were for data in an identified one of files residing primarily on an identified internal, removable, or external media;

(b) first testing for each intercepted file-closing attempt, to verify that the identified media on which the to-be-closed file primarily resides is currently available, and if not, updating local records which track the current availability of the identified media to indicate the current non-availability of the media;

(c) second testing for each intercepted file-closing attempt, to determine if access constraining control information is available internally for the identified file;

(d) if said second testing shows that the access constraining control information is not available in an internal and physically-secure storage area, determining explicitly or implicitly if the missing, access constraining control information must be locally present for allowing the intercepted file-closing request to complete normally, and if the missing information is necessary, blocking the intercepted file-closing request from completing normally in response to the intercepted file-closing request.

12. (Original) The instructions conveying means of Claim 40 and wherein said nonresident file-closing method further comprises:

(e) third testing the locally-present, access constraining control information for the to-be-closed file to determine if the access constraining rules for the identified file permit a current attempt to close the file; and

(f) blocking the intercepted file-closing request from completing normally if said third testing step (e) indicates the locally-present, access constraining control information for the to-be-closed file do not permit a current attempt to close the file.

13. (Original) The instructions conveying means of Claim 41 and wherein said nonresident file-closing method further comprises:

(g) determining if other local, application programs are still using the localized file copy, and if so, fooling the file-closing requesting application program into to thinking the nonresident original of the identified file has been closed, even though said nonresident original has not yet been closed.

14. (Original) The instructions conveying means of Claim 42 and wherein the nonresident file-closing method further comprises:

(h) if no other local, application programs are still using the localized file copy, determining if the localized file copy has been modified locally; and

(i) if said determining step (h) shows that the localized file copy has not been modified locally, allowing the intercepted file-closing request to complete normally, thereby causing a file-close action to occur for the nonresident file identified in a counterpart, file-opening request.

15. (Original) The instructions conveying means of Claim 43 and wherein the nonresident file-closing method further comprises:

(j) in conjunction with said step (i) of allowing the requested file-close action to occur for the nonresident file, deleting the localized file copy.

16. (Original) The instructions conveying means of Claim 44 and wherein the nonresident file-closing method further comprises:

(k) in conjunction with said step (i) of allowing the requested file-close action to occur for the nonresident file, determining if any other, temporarily localized filed copies (TTL'ed files) are logically associated with the localized copy of the access constraining rules of the to-be-closed file, and if not, deleting the localized copy of the access constraining rules of the to-be-closed file.

17. (Original) The instructions conveying means of Claim 43 and wherein the nonresident file-closing method further comprises:

(j) if said determining step (h) shows that the localized file copy has been modified locally, overwriting the modified local copy to the nonresident, original location before allowing the intercepted file-closing request to complete normally, thereby causing a file-close action to

occur for the nonresident file identified in a counterpart, file-opening request only after the nonresident file has been updated in accordance with the locally-made modifications.

18. (Original) The instructions conveying means of Claim 41 and wherein the nonresident file-closing method further comprises:

(e) in response to a denial of the requested file-closing, posting a correspondingly security alert message.

19. (Original) In an automated machine for executing one or more application programs, where the application programs access file data of a plurality of locally and externally stored files by causing interceptable file-OPEN requests and file-CLOSE requests to be sent to an operating system of said machine, and where data within a subset of the plurality of stored files is encrypted or otherwise access constrained; an automatic access constraining control mechanism comprising:

(a) OPEN intercept means for intercepting said interceptable file-OPEN requests;

(b) selective OPEN continuance means, responsive to the OPEN intercept means, for determining whether an intercepted file-OPEN request is requesting an open of a file for which the request is to be denied based on associated access constrain rules;

(c) local-use tracking means , responsive to the selective OPEN continuance means, for determining whether a localized copy of a to-be-opened, nonresident file, and a localized copy of nonresident access constraining rules associated with the to-be-opened, nonresident file, are already present in the machine, and if so, for allowing the intercepted file-OPEN request to continue on its way to the operating system such that the localized file copy will be accessed if so permitted by the localized copy of nonresident access constraining rules;

(d) CLOSE intercept means for intercepting said interceptable file-CLOSE requests; and

(e) selective CLOSE continuance means, responsive to the OPEN intercept means, for determining whether an intercepted file-CLOSE request is requesting a closing of a file for which the CLOSE request is to be denied based on associated access constrain rules.

20. (Original) The instructions conveying means of Claim 41 and wherein said nonresident file-closing method further comprises:

(g) determining if the to-be-closed file is a special-use one such that, even if there are no other local, application programs still using the localized file copy, still fooling the file-closing requesting application program into to thinking the nonresident original of the identified file has been closed, even though said nonresident original has not yet been closed because it is later slated for special-use by an application program that has not yet started using the localized file copy.